02. Identificación de riesgos prioritarios y medidas correctivas.

Ejemplo sencillo de matriz de riesgos (Recordatorio del Módulo 1):

Activo	Amenaza	C	I	D	A	T	Impacto Total	Probabilidad	Nivel de Riesgo	Medida de mitigación
Base de datos	Acceso no autorizado	Alto	Alto	Medio	Medio	Alto	13	Media	26	Implementar control de acceso y cifrado
Servidor web	Ataque DDoS	Bajo	Medio	Alto	Medio	Bajo	9	Alta	27	Usar firewall y balanceador de carga
Documentación interna	Pérdida por error humano	Medio	Alto	Bajo	Bajo	Medio	9	Media	18	Copias de seguridad y formación del personal
Correo corporativo	Phishing	Alto	Medio	Bajo	Alto	Medio	11	Alta	33	Filtro antiphishing y concienciación
Copias de seguridad	Robo físico	Alto	Alto	Alto	Bajo	Bajo	11	Baja	11	Almacenamiento seguro y cifrado

(Alto=3, Medio=2, Bajo=1) (Impacto total = C+I+D+A+T) (Nivel de riesgo = Impacto total * probabilidad)

02. Identificación de riesgos prioritarios y medidas correctivas.

Ejemplo básico de cálculo de nivel de riesgo: caso “brecha de datos personales”

Supuestos de nuestra metodología de análisis de riesgos:

El cálculo del riesgo se haría con la fórmula:

Riesgo = Probabilidad × Impacto"

Donde:

- Probabilidad: frecuencia o posibilidad de que ocurra (escala 1-5).
- Impacto: consecuencia si ocurre (escala 1-5).
- Riesgo: bajo, moderado, alto, crítico.

1. Cálculo del **riesgo inherente** en la situación inicial:
   Probabilidad: 4 (Ej. procesos manuales, sin cifrado)
   Impacto: 5 (Ej. sanciones ente regulador, reputación)
   Riesgo inherente = 20 (Alto)

Riesgo	Probabilidad	Impacto	Riesgo inherente
Brecha datos personales expuestos	4	5	20

2. Medidas de seguridad o controles:
   Cifrado de datos
   Políticas de acceso
   Auditorías periódicas

3. Cálculo del **riesgo residual** tras medidas de seguridad:
   Probabilidad: 2
   Impacto: 4
   Riesgo residual = 8 (Moderado)

Riesgo	Probabilidad	Impacto	Riesgo residual
Brecha datos personales expuestos	2	4	8

02. Identificación de riesgos prioritarios y medidas correctivas.

Aceptación del riesgo

Las metodologías de gestión de riesgos definen tablas para valorar los impactos, las frecuencias y los niveles de riesgo.

Por ejemplo NITS (NIST SP 800-30 Rev. 1 Guide for Conducting Risk, metodología para la gestión de riesgos) dispone en una tabla I-3 la interpretación del nivel de riesgo:

Valores cualitativos	Valores semicuantitativos		Escala de evaluación del impacto
Muy alto	96-100	10	Riesgo Muy Alto significa que se podría esperar que una amenaza tenga múltiples efectos adversos graves o catastróficos en las operaciones, los activos, las personas, otras organizaciones o la Nación.
Alto	80-95	8	Riesgo Alto significa que se podría esperar que una amenaza tenga un efecto adverso grave o catastrófico en las operaciones, los activos, las personas, otras organizaciones o la Nación.
Moderado	21-79	5	Riesgo Moderado significa que se podría esperar que una amenaza tenga un efecto adverso grave en las operaciones, los activos, las personas, otras organizaciones o la Nación.
Bajo	5-20	2	Riesgo Bajo significa que se podría esperar que una amenaza tenga un efecto adverso limitado en las operaciones, los activos, las personas, otras organizaciones o la Nación.
Muy bajo	0-4	0	Riesgo Muy Bajo significa que se podría esperar que una amenaza tenga un efecto adverso insignificante en las operaciones, los activos, las personas, otras organizaciones o la Nación.

Y por ejemplo una organización podría determinar que:

Muy alto Alto Moderado	No aceptables. (hay que tratar el riesgo – PTR)
Bajo Muy bajo	Aceptables (se puede tratar el riesgo)

Pero **es la política de la empresa en relación con los riesgos, la que determinará qué riesgos son aceptables y cuáles no**.